

# Cyber Security and Autonomous Systems for the Offshore Wind Environment Report

PN000844-RPT-006 OLTER Project 4



Author: Ruth Wilson-Nash

Date: 02/05/2025

In partnership with:



## DISCLAIMER

---

Whilst the information contained in this report has been prepared and collated in good faith, ORE Catapult makes no representation or warranty (express or implied) as to the accuracy or completeness of the information contained herein nor shall we be liable for any loss or damage resultant from reliance on same.

## DOCUMENT HISTORY

---

Revision	Date	Prepared by	Checked by	Approved by	Revision History
<b>Rev 1</b>	22 April 2025	R Wilson-Nash	J Walker A McCallien	K York	First release
<b>Rev 2</b>	02 May 2025	R Wilson-Nash	J Walker	K York	Minor wording amendments following OLTER review

Field	Detail
<b>Report Title</b>	Cyber Security and Autonomous Systems for the Offshore Wind Environment Report
<b>Status</b>	Public
<b>Document Reference</b>	PN000844-RPT-006

## PREFACE

---

This report forms part of the wider OLTER (Offshore Low Touch Energy Robotics & Autonomous Systems) project where the aim is to deliver a Robotics and Autonomous Systems (RAS) service, to scale and commercialise robotics for use in offshore energy environments. The purpose of this report is to explore the types and future of autonomous systems, general cyber security landscape, and how these interact in the offshore wind environment. The report focuses on offshore wind, however many of the points discussed are relevant across other offshore energy sectors. In addition to the report a toolkit [1] has been developed to provide decision-makers with a resource to assess the cyber security risk of using autonomous systems around the wind farm.

The offshore wind industry is growing at a fast rate and, particularly in the UK, installing wind farms further from shore. This increases the challenges associated with all activities, and particularly during the operations and maintenance phase. The use of RAS is becoming increasingly prevalent with the aims to improve safety, reduce costs and reduce emissions.

Autonomous systems are those with the capability of completing operations independently. There are different degrees of autonomy that systems can operate in, with humans taking less control as confidence is gained in the ability of the system to complete operations safely. Within offshore wind, the RAS operating areas include aerial, sea surface and subsurface. Remotely operated systems are currently in use, such as unmanned aerial vehicles (UAV), uncrewed surface vehicles (USV) and remotely operated vehicles (ROV). However, there are very few autonomous systems in operation due to the regulatory landscape, technology development levels and industry confidence. This is expected to change in the future as the offshore wind industry becomes more dependent on RAS, however much needs to be understood by offshore wind developers and owner operators to build confidence. One area of concern is the cyber security risk posed by autonomous systems operating in and around wind farms.

Cyber security affects all industries, and this report explores key areas such as standards, best practice, attack types and attack motivations. In relation to autonomous systems specific areas of data security, supply chain security, wind farm network interfacing, software and system testing are discussed. The key risks associated with the use of autonomous systems are highlighted and it should be noted that many of these risks are synonymous with the risks posed by remotely operated systems already in use. The key factors affecting risk and mitigations are also explored. These are further expanded upon in the accompanying toolkit [1] to support decision-makers.

Final recommendations apply to technology developers and decision-makers (wind farm developers and owner operators) as well as highlighting future priority areas.

# CONTENTS

---

- 1 Introduction..... 1**
  - 1.1 Overview .....1
  - 1.2 Purpose .....1
  - 1.3 Aims and Objectives of the Project.....1
  - 1.4 Scope .....2
  - 1.5 Stakeholder Engagement .....2
- 2 Background..... 3**
- 3 Autonomous Systems Overview ..... 4**
  - 3.1 Degrees of Autonomy .....4
  - 3.2 Types of Autonomous Systems .....6
  - 3.3 Regulations.....8
  - 3.4 Use of Autonomous Systems in Offshore Wind..... 10
  - 3.5 Understanding of Autonomous Systems in the Offshore Wind Industry ..... 14
- 4 Cyber Security Overview .....14**
  - 4.1 Relevant Standards and Regulations..... 14
  - 4.2 Best Practice..... 15
  - 4.3 Attack Types ..... 19
  - 4.4 Detecting an Attack..... 21
- 5 Cyber Security and Autonomous Systems .....22**
  - 5.1 Relevant Standards, Regulations and Guidance ..... 22
  - 5.2 Cyber Security and Autonomous Systems Best Practice..... 23
  - 5.3 Cyber Security Risks ..... 26
  - 5.4 Cyber Security Risk Mitigations..... 29
- 6 Conclusion .....30**
- 7 Recommendations .....30**
  - 7.1 Technology Developers..... 30
  - 7.2 Decision-Makers..... 30

7.3 Future Priority Areas ..... 31

**8 References.....32**

**Appendix 1 List of Useful Resources.....37**

**LIST OF FIGURES**

---

Figure 1 Stakeholder engagement by category ..... 2

Figure 2 Wind farm development stages and the categories used for Table 2 ..... 4

Figure 3 Degrees of autonomy classification comparison between the IMO and three classification societies [6] ..... 5

Figure 4 Approach to degrees of autonomy by Bureau Veritas [7] ..... 5

Figure 5 Types of robotics and autonomous systems considered (Not to actual size). [9], [10], [11], [12], [13] ..... 6

Figure 6 XOCEAN X-03 USV [20] (left) and Fugro Blue Essence USV [21] (right) ..... 7

Figure 7 Classifications of autonomous maritime system and autonomous ship types [22] ..... 7

Figure 8 Possible outlook for the use of autonomous systems in offshore wind ..... 11

Figure 9 NCSC 10 steps to Cyber Security infographic [35]..... 15

Figure 10 Cyber security good practice ..... 16

Figure 11 The CIA triad [36]..... 17

Figure 12 Vulnerability management process [43]. ..... 18

Figure 13 Attack detection timescales across each region ..... 21

Figure 14 Best Practice categories of Cyber Security and Autonomous Systems ..... 24

**LIST OF TABLES**

---

Table 1 Project scope table ..... 2

Table 2 Distances from shore and total capacity of UK wind farms at different stages of development (calculated from 4C Offshore data)..... 3

Table 3 Regulations and standard for offshore autonomous systems [28] ..... 9

Table 4 Possible activities for autonomous systems across the lifecycle of an offshore wind farm .... 12

Table 5 Relevant standards and regulations for cyber security ..... 14

Table 6 Attack Types [44], [45], [46] ..... 19

Table 7 Types of attackers and their motivations [47]..... 20

Table 8 Relevant standards and regulations for the cyber security of autonomous systems ..... 22

Table 9 UR E26 and UR E27 scope of applicability [50], [51] ..... 23

Table 10 Perceived cyber security risks..... 27

Table 11 Factors affecting cyber security risks..... 28

Table 12 Cyber security risk mitigations ..... 29

## NOMENCLATURE

---

AI	Artificial Intelligence
ASV	Autonomous surface vehicle
AUV	Autonomous underwater vehicle
BV	Bureau Veritas
BVLOS	Beyond visual line of sight
CAA	Civil Aviation Authority
CBS	Computer-based systems
CHERI	Capability Hardware Enhanced RISC Instructions
CIA	Confidentiality, Integrity and Availability
CTV	Crew transfer vessel
DDoS	Distributed-denial-of-service
DoS	Denial-of-service
EMEA	Europe, the Middle East and Africa
FOWT	Floating offshore wind turbine
GDPR	General Data Protection Regulation
IATA	International Air Transport Association
IMO	International Maritime Organization
IoT	Internet of Things
JAPAC	Japan and Asia Pacific
MCA	Maritime & Coastguard Agency
MITM	Man-in-the-middle

ML	Machine learning
NCSC	National Cyber Security Centre
NOC	National Oceanography Centre
O&G	Oil and Gas
O&M	Operations and Maintenance
OLTER	Offshore Low Touch Energy Robotics & Autonomous Systems
OWF	Offshore wind farm
QMS	Quality management systems
RAS	Robotics and Autonomous Systems
RF	Radio frequency
ROC	Remote operation centre
ROV	Remotely Operated Vehicle
SOLAS	Safety of Life at Sea
SOV	Service operation vessel
UAV	Unmanned aerial vehicles
USV	Uncrewed surface vehicles
UUV	Uncrewed underwater vehicles
VLAN	Virtual local area network
VLOS	Visual line of sight
WTG	Wind turbine generator

# 1 INTRODUCTION

---

## 1.1 Overview

This report forms part of the wider OLTER (Offshore Low Touch Energy Robotics & Autonomous Systems) project where the aim is to deliver a Robotics and Autonomous Systems (RAS) service, to scale and commercialise robotics for use in offshore energy environments [2]. There are four key areas of this project which include:

1. Establishing a new Testing and Assurance Centre.
2. Demonstrating a Shared Data Platform and Hi-Fidelity Digital Twin.
3. Delivering "art of the possible" offshore RAS demonstrations.
4. Creating a Knowledge Portal.

This report sits within the Knowledge Portal which has been developed to share resources for the RAS community.

In addition to the report, a toolkit [1] has been developed to provide decision-makers with a resource to assess the cyber security risk of using autonomous systems around the wind farm. The toolkit should be viewed in conjunction with this report.

## 1.2 Purpose

The purpose of this report is to explore the types and future of autonomous systems, general cyber security landscape, and how these interact in the offshore wind environment. There is a focus on stating possible risks and mitigations which should be viewed alongside the toolkit. While the specific use case explored is offshore wind, the risks, mitigations and toolkit can be applied to other offshore energy sectors.

The report is aimed at industry decision-makers and technology developers. The decision-makers could be wind farm developers and owner-operators. Technology developers are supported in understanding what could be done to improve the likelihood of technology adoption from a cyber security perspective.

## 1.3 Aims and Objectives of the Project

The aims of this project are to:

- Identify the requirements for cyber security to ensure safe and secure operations of autonomous systems within sensitive sites.
- Support the adoption of new technologies by providing a toolkit to decision-makers identifying severity, likelihood and failure mitigations, whether caused by malicious action or accident (see toolkit [1]).

The objectives of this project are to:

- Assess industry concerns around autonomous systems and cyber security.

- Define cyber security attack mechanisms.
- Establish the potential consequences of an attack at business, wind farm, local and national level (see toolkit [1]).
- Define criteria and acceptance levels for industry in relation to the cyber threat. Providing a toolkit for decision-makers (see toolkit [1]).
- Recommend priority areas for future work.

### 1.4 Scope

Table 1 defines the areas that have been set as in or out of scope for this project.

Table 1 Project scope table

In Scope	Out of Scope
<ul style="list-style-type: none"> <li>• Autonomous systems including aerial, surface and subsea crafts</li> <li>• In/on/near key assets – Turbines, foundations, substations, cables</li> <li>• Focus on offshore wind with a short review of the automotive and aerospace industries</li> <li>• Malicious and accidental actions.</li> <li>• Attack consequences – business, local and national</li> </ul>	<ul style="list-style-type: none"> <li>• Windfarm control systems</li> <li>• Systems operating outside of these areas</li> <li>• Other industries</li> <li>• Reasons for attacks – mentioned but not expanded on</li> </ul>

### 1.5 Stakeholder Engagement

Stakeholder engagement was conducted in order to understand the thoughts of the industry, gain insights into best practice and build a better picture of how autonomous systems will interact with wind farms from a cyber security perspective. Twenty stakeholder engagement sessions were held involving 41 individuals and spread across the categories shown in Figure 1. The author would like to thank all those who have participated in this engagement.

Stakeholder Engagement Company Categories

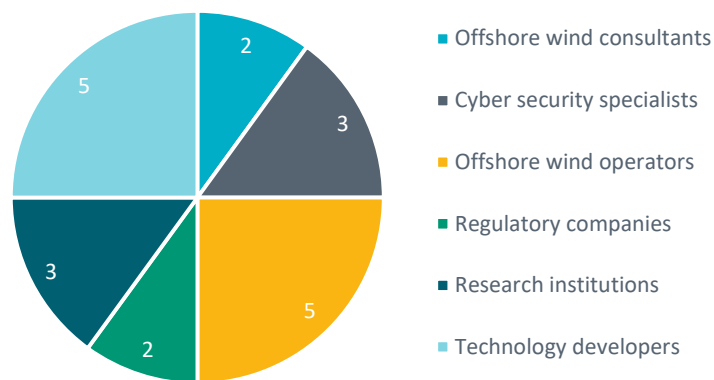


Figure 1 Stakeholder engagement by category

## 2 BACKGROUND

The offshore wind industry is expected to see high levels of growth in the next two decades and there are a number of changing factors that will affect the future of the industry. The water depth and distance of wind farms from shore will have a direct impact on type of turbine foundation used, the operation and maintenance (O&M) strategies implemented, and the activities associated with these. Table 2 shows the different distances from shore of UK wind farms at varying stages of construction and operation (refer to Figure 2). Of the 16 GW currently installed, fully commissioned and therefore operational, the average distance from shore is 23 km with a maximum distance of 115 km. When considering the planned wind farms with consent authorisation that are not yet fully commissioned the maximum distance increases to 207 km with an average of 65 km. There are also wind farms in the concept/early planning stages up to 261 km from shore. This distance has the following implications:

- The O&M strategy will diversify.
  - Most wind farms currently transfer technicians to turbines on a daily basis via a crew transfer vessel (CTV). However, as wind farms move further from shore this becomes uneconomical and a strategy housing technicians on service operation vessels (SOVs) remaining offshore for 2 weekly periods is more likely to be utilised.
- Offshore conditions are often more challenging and dangerous to operate in, reducing the opportunity to access turbines and complete maintenance tasks.
- Water depths will increase.
  - Deeper waters are impractical for traditional fixed bottom turbines. Wind farms in these areas will likely use floating offshore wind turbines (FOWTs) where the turbine foundation floats and is anchored to the seabed via mooring lines.
  - FOWTs will require additional subsea inspections of mooring lines, anchors, floating platforms and dynamic cables.

Table 2 Distances from shore and total capacity of UK wind farms at different stages of development (calculated from 4C Offshore data)

	Wind farm development categories		
	1 - Fully Commissioned	2 - Consent authorised to under construction	3 - Concept/early planning to fully commissioned
Min distance (km)	2	2	2
Max distance (km)	115	207	261
Ave distance (km)	23	65	50
Total capacity (GW)	16	21	81

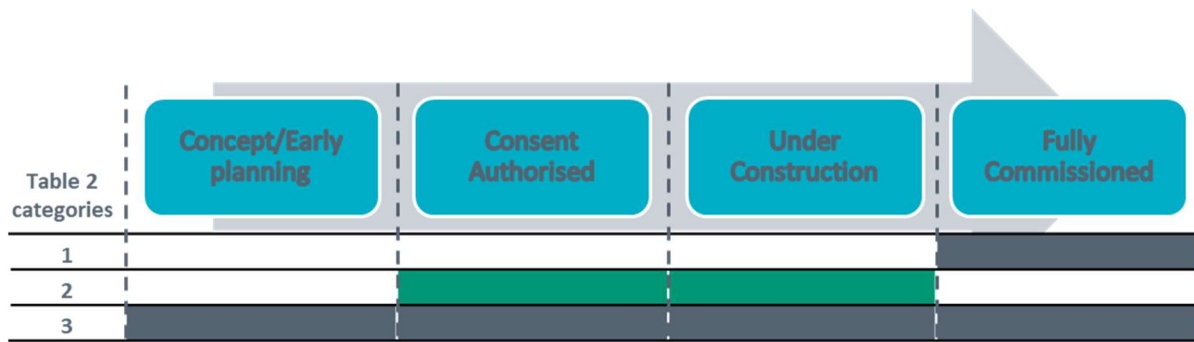


Figure 2 Wind farm development stages and the categories used for Table 2

Current practice requires human intervention to captain vessels, undertake surveys and complete inspections and repairs, amongst other activities. Two of the industry aims are increased safety by reducing the number of trips required offshore and level of human intervention, and improved efficiency of tasks to reduce costs. As the industry grows and moves further offshore these will assume increasing importance, and one solution is the increased use of RAS. Some robotics, such as unmanned aerial vehicles (UAVs) are widely used in the industry for tasks such as performing blade inspections. However, there is increased opportunity for a greater variety of robotics with greater levels of autonomy to be utilised.

### 3 AUTONOMOUS SYSTEMS OVERVIEW

#### 3.1 Degrees of Autonomy

Autonomy refers to the ability of a person, or in this case robot, to be self-governed, free from excessive external control and independent [3]. Autonomous systems are defined as “systems with the capability to complete autonomous operation with independent onboard decision making while adhering to a set of rules which ensure safety and self-certification” [4]. Within the context of robotic autonomous systems these may have full or partial autonomy. Whilst autonomous systems are often discussed as a single category it should be noted that individual systems can have differing degrees of autonomy. The International Maritime Organization (IMO) identifies four degrees of autonomy for ships [5]:

- Degree 1: Ship with automated processes and decision support.
- Degree 2: Remotely controlled ship with seafarers on board.
- Degree 3: Remotely controlled ship without seafarers on board.
- Degree 4: Fully autonomous ship.

The degrees of autonomy are based on the decision-making ability of the system and level of human intervention required. Across the industry, different classification societies have taken varying approaches to autonomy [6]. A comparison of these is shown in Figure 3, with the approach taken by Bureau Veritas (BV) provided in more detail in Figure 4.

IMO	Lloyd’s Register	Bureau Veritas	DNV
	AL 0	Degree A0	M (manually operated)
Degree 1	AL 1	Degree A1	DS
Degree 2	AL 2	Degree A2	
Degree 3	AL 3	Degree A3	
	AL 4		DSE
Degree 4	AL 5	Degree A4	SC
			A

Figure 3 Degrees of autonomy classification comparison between the IMO and three classification societies [6]

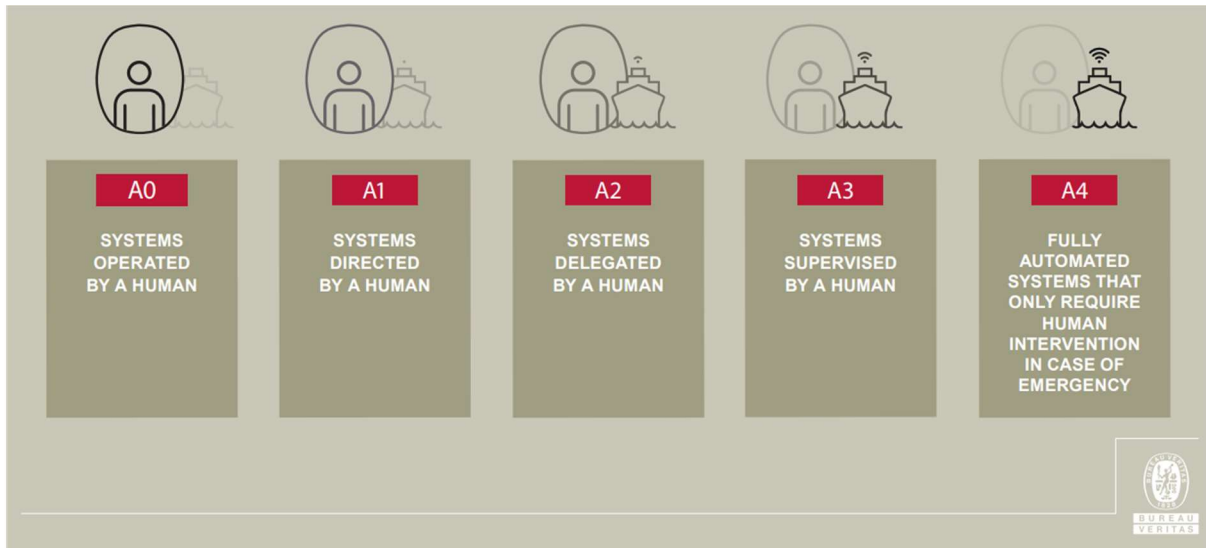


Figure 4 Approach to degrees of autonomy by Bureau Veritas [7]

As confidence increases in the ability of the system to make safe and considered decisions, the level of human intervention can be reduced. For example, using the BV approach, an A2 degree may allow a system to suggest the action it wishes to take but await agreement from the human operator before proceeding. Once confidence is built in the system and the operator agrees with all decisions, it could be upgraded to an A3 where the system would be supervised by an operator who is informed of all decisions as it undertakes a task and the operator would be able to step in and take over if necessary. Once confidence is built in the system and the operator is not required to step in, it may be moved up to an A4 degree where an operator is only informed in case of emergency. Each of these steps and change in degree of autonomy requires the criteria set out in NI 641 [8] to be met.

### 3.2 Types of Autonomous Systems

For the purpose of this report marine and aerial autonomous systems have been considered. Figure 5 shows the different types of systems discussed within this report in relation to their operational area.

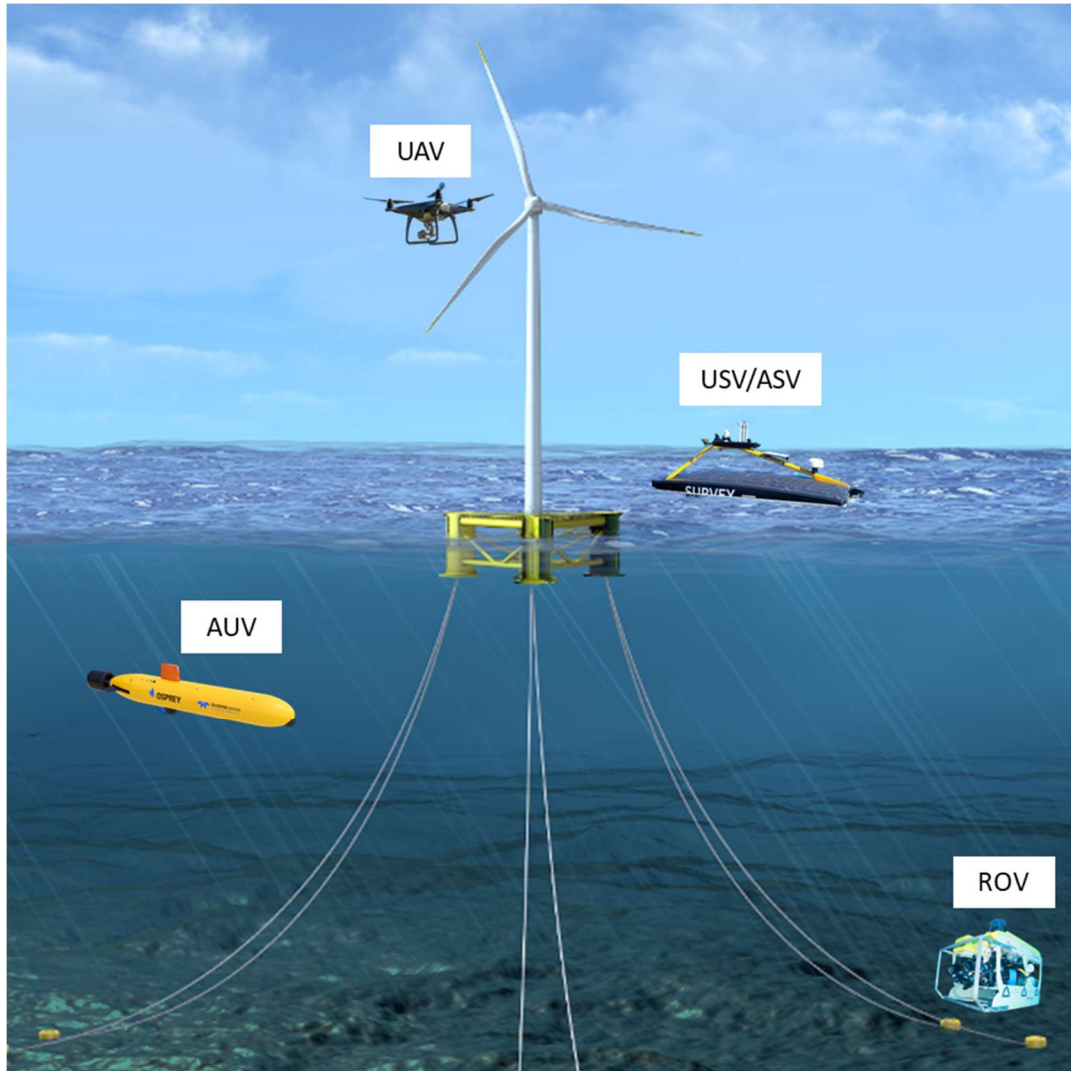


Figure 5 Types of robotics and autonomous systems considered (Not to actual size). [9], [10], [11], [12], [13]

UAVs have been commonplace in offshore wind for many years, with the main focus on completing external blade inspections, replacing the need for rope access technicians to complete this task. The development of sensors and uses onshore is translating into wider uses of UAVs offshore, such as marine mammal and bird monitoring, water quality surveys and metocean surveys [14]. UAVs are currently manually piloted with the capability to perform some autonomous tasks such as tracking a wind turbine blade during inspection. Operators are typically on a vessel within visual-line-of-site (VLOS) of the UAV. Although autonomous drones are being used for some applications, such as the delivery of medical supplies in London by Apian [15], there are barriers to wider use. The operation of UAVs beyond-visual-line-of-site (BVLOS) of the operator is a regulatory challenge the Civil Aviation Authority (CAA) is working to better define, with offshore wind being a focus area [16]. Autonomous drones, without the need for manual operation or constant supervision, are unlikely to become commonplace in the offshore wind industry until the regulatory framework is updated.

Uncrewed surface vessels (USVs) are becoming more commonplace within the offshore wind industry with these being covered by the Maritime & Coastguard Agency (MCA) in their code of practice The Workboat Code Edition 3 [17], and Marine Guidance Notices MGN 702 [18] and MGN 705 [19]. Figure 6 shows examples of USVs currently operating within the industry. Although these are currently operated from a remote operation centre (ROC) it is possible the technology is ready to take on further degrees of autonomy if regulations allow.

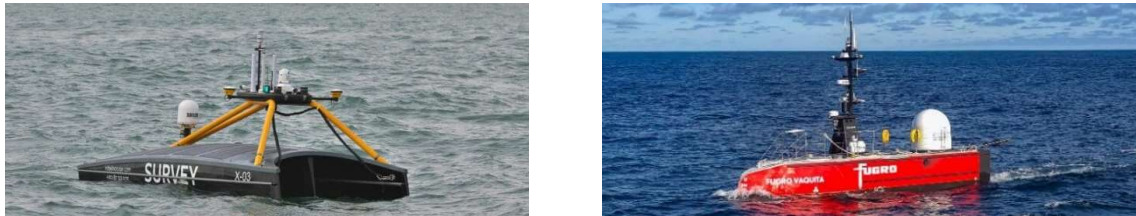


Figure 6 XOCAN X-03 USV [20] (left) and Fugro Blue Essence USV [21] (right)

The different classifications of marine autonomous vehicles are shown in Figure 7. The cyber security risks associated with autonomous surface and underwater vehicles (ASV/AUV) are likely to be very similar to those of uncrewed surface and underwater vehicles (USV/UUV). This is on the basis that much of the technology is similar and the effects of an attack are likely to be the same. For example, if an ASV and USV are of a similar size, material and operational speed, the physical damage they could cause to a turbine or vessel in the event of a cyber-attack is likely to be similar.

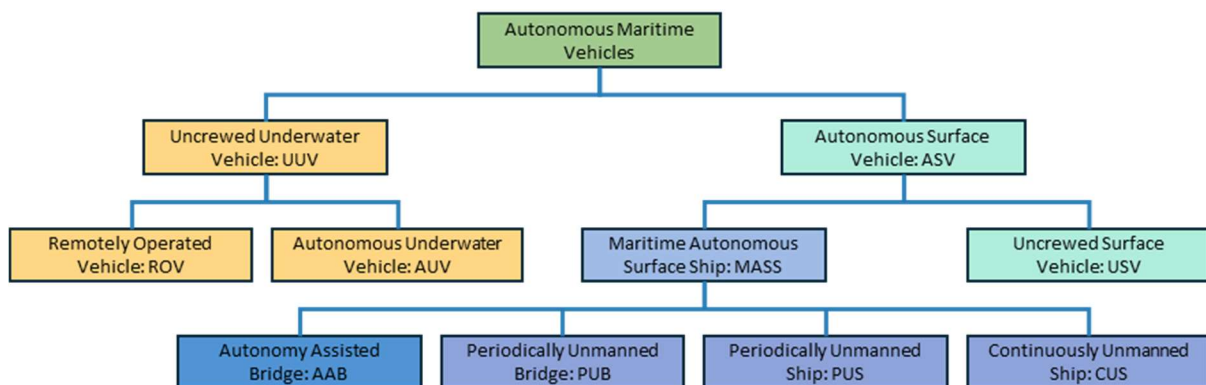


Figure 7 Classifications of autonomous maritime system and autonomous ship types [22]

Remotely operated vehicles (ROVs) are typically pilot operated from an ROC. As the technology develops parts of the operation are becoming more automated, such as navigation to specific locations, moving the degree of autonomy from A1 to A2 (see Figure 4). Current autonomy appears to be focused on the navigation aspect and observation/inspection ROVs as opposed to work-class ROVs, due to the added complexity of work-class ROVs. Current practice is for ROVs to be tethered to a surface vessel or resident system for power, control and data transfer purposes. From a cyber security perspective, the hardwired tethered connection provides excellent protection of the system with this link practically impossible to hack. However, untethered ROVs are also on the horizon with companies such as Greensea Systems developing software that demonstrates successful tetherless missions [23]. The cyber security risks of the systems must be carefully considered to reduce the likelihood of successful attacks.

In addition to the operation of autonomous systems, additional infrastructure is likely to be needed to support autonomous systems offshore. For example, charging and data upload stations may be required for autonomous systems performing long operations offshore. These represent a different challenge with the possibility of third-party devices docking in them.

### 3.3 Regulations

The development of regulations for aerial and marine systems has long been a “chicken and egg” scenario with regulators wanting to see operations so they can understand the risks, and operators requiring regulations to understand what they are aiming for. Currently most used autonomous systems are in the defence industry, and therefore exempt from standard regulation, or for research. The National Oceanography Centre (NOC) [24] and UK Marine Industries Alliance [25] set out good practice for operating autonomous systems, which include:

- Ensuring vessels have clear identification features such as the operator’s name and contact details.
- Issuing a notice to mariners if operating in fishing areas, near shipping lanes or in other countries requiring this.
- Avoiding areas of high vessel traffic to reduce the risk of collision.
- Avoiding coastal areas to keep away from regions with heavy tides.
- Seeking approval from the sovereign state if operating outside UK waters and in exclusive economic zones.

For the widespread use of autonomous and unmanned systems to be adopted, regulations and standards are needed. These are to support the development and understanding of safe systems, thus improving industry confidence. However, for regulatory development to be considered there must first be a need and then experience gained to ensure regulations will be fit for purpose. For example, USVs have been utilised for a number of years, with XOcean’s first offshore wind farm survey of Greater Gabbard in 2020 [26] and data harvesting operation at BP’s Machar field in the North Sea in 2019 [27]. Despite these operations, USVs (or remotely operated unmanned vessels as they are referred to) were only added to the Workboat Code in December 2023 when Edition 3 was released.

With respect to autonomy the regulatory space is relatively immature. Table 3 highlights some current regulations and standards that have relevance to autonomous systems (left column) and those in development that are specific to autonomous systems (right column).

Table 3 Regulations and standard for offshore autonomous systems [28]

<b>Applicable regulations and standards relevant to autonomous systems</b>	<b>Current and developing standards and regulations specific to autonomous systems</b>
<ul style="list-style-type: none"> <li>• The Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2011</li> <li>• CAA CAP 393: Regulations made under powers in the Civil Aviation Act 1982 and the Air Navigation Order 2016</li> <li>• IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems</li> <li>• RTCA DO-178B/C: Software Considerations in Airborne Systems and Equipment Certification</li> <li>• SAE ARP4754 - Guidelines for Development of Civil Aircraft and Systems</li> <li>• ISO 26262: Road Vehicles - Functional Safety</li> <li>• ISO 10218: Safety Requirements for Industrial Robots</li> <li>• ISO 18646: Robotics - Performance criteria and related test methods for service robots</li> <li>• ISO 20218: Robotics - Safety design for industrial robot systems</li> </ul>	<ul style="list-style-type: none"> <li>• Maritime UK: Maritime Autonomous Surface Ships Industry Conduct Principles &amp; Code of Practice</li> <li>• UK Marine Industries Alliance (MIA): Industry Code of Conduct for Maritime Autonomous Systems</li> <li>• Lloyd’s Register - ShipRight Procedure for assignment of digital descriptive notes for autonomous and remote access ships</li> <li>• Lloyd’s Register - Code for Unmanned Marine Systems</li> <li>• CAP 722: Unmanned Aircraft System Operations in UK Airspace – Guidance</li> <li>• BS 8611 - Robots and robotic devices. Guide to the Ethical Design and Application of Robots and Robotic Systems</li> <li>• IEEE 7001 - Transparency of Autonomous Systems</li> <li>• IEEE 7007 - Ontological Standard for Ethically Driven Robotics and Automation Systems</li> <li>• IEEE P7008 - Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems</li> <li>• IEEE 7009 - Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems</li> <li>• IEEE 7010 - Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being</li> <li>• IEEE P7014 - Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems</li> <li>• ISO/TS 15066: Robots and robotic devices - Collaborative robots</li> </ul>

### 3.4 Use of Autonomous Systems in Offshore Wind

The use of autonomous systems will depend greatly on the development of technology and regulations. Figure 8 looks at the possible timeline for this, and

Table 4 highlights some of the activities to which autonomous systems may be applied across the lifecycle of an offshore wind farm.

#### 3.4.1 Current

Current use of autonomous systems is limited due to technological and regulatory barriers. Most systems are either operated by humans (A0, with operators onboard) or directed by humans (A1, with operators at an ROC or nearby).

#### 3.4.2 Short-term Future (<5yrs)

In the short-term future it is expected systems will start to move into more advanced levels of autonomy without reaching full autonomy (move into A2 and possibly A3). The advancement of these may be restricted by regulatory requirements.

#### 3.4.3 Long-term Future (>5yrs)

In the long-term future, fully autonomous systems are likely to become more mainstream commercially with many systems able to operate with full autonomy (A4).

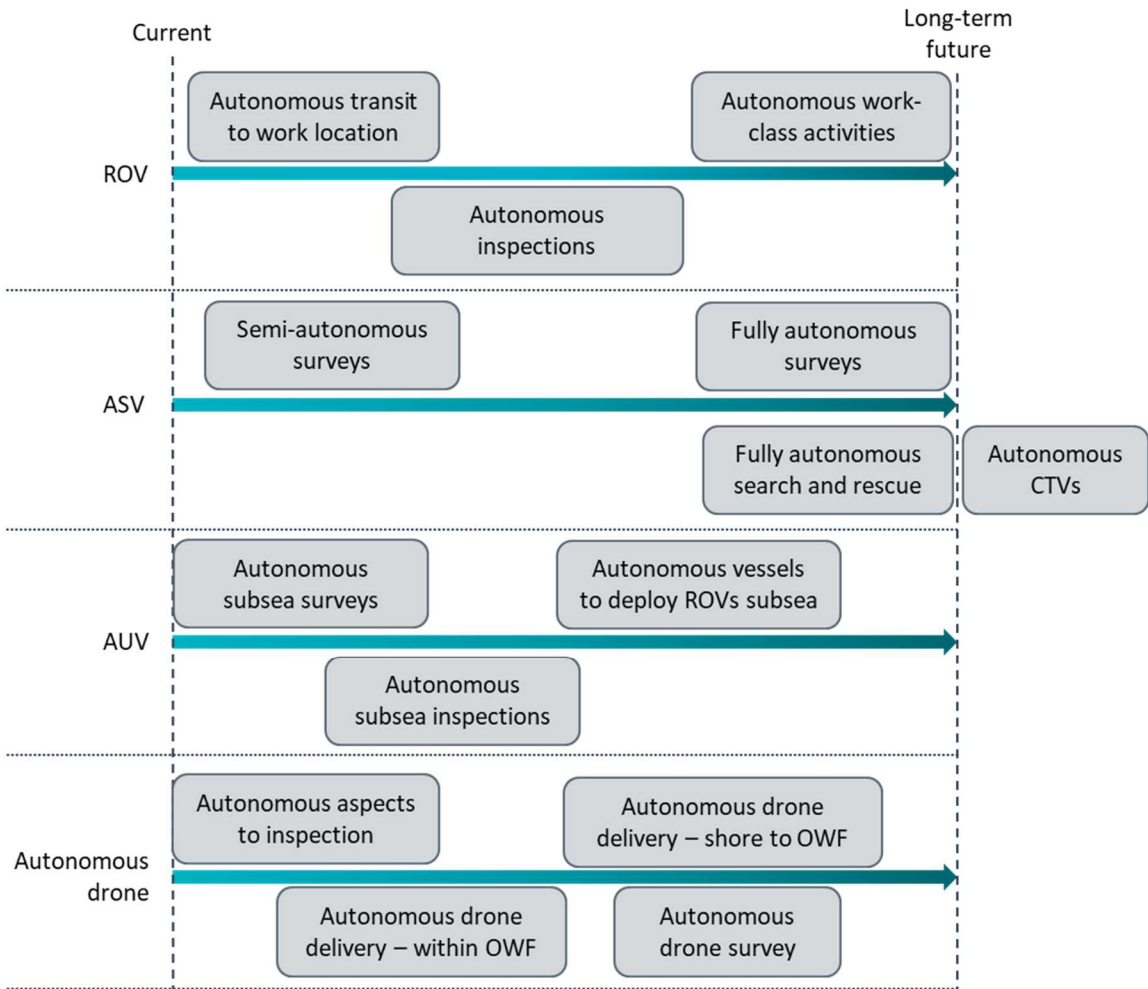


Figure 8 Possible outlook for the use of autonomous systems in offshore wind

Table 4 Possible activities for autonomous systems across the lifecycle of an offshore wind farm

Lifecycle	Category	Survey/activity	ROV	ASV	AUV	Auto Drone
Development & Consenting	Environmental Surveys	Benthic Surveys	Y	Y	Y	
		Ornithological surveys				Y
		Marine Mammal Surveys		Y	Y	Y
	Geological and Hydrographical	Geophysical survey		Y		
Construction	Pre-construction prep	Pre-construction Survey - UXO/boulder/debris assessment	Y	Y	Y	
		Seabed Preparation - boulder/UXO removal and assessment	Y	Y	Y	
		Deep water route survey		Y		
	Foundation Installation	Pile Driving assessment	Y			
		Grouting assessment	Y			
		Mooring (Floating Foundations) assessment	Y			
		Scour Protection survey	Y			
	Cable Installation	Grapnel Run survey	Y	Y	Y	
		Cable Pull-in monitoring	Y		Y	
		Cable Burial assessment	Y		Y	
O&M	Environmental monitoring	Marine Life Monitoring		Y		
		Ornithological surveys				Y
		Seabed Monitoring	Y		Y	
	Support Structure inspection and Repair	Fixed Foundation (and subsea structures)	Y		Y	
		Floating Substructure and Mooring system	Y		Y	
		Scour monitoring	Y		Y	

Lifecycle	Category	Survey/activity	ROV	ASV	AUV	Auto Drone
	Turbine inspection	Blades and tower inspection				Y
	Cable inspection and repair	Fixed	Y	Y	Y	
		Floating	Y	Y	Y	
	Navigation aids inspection	Navigation aids inspection				Y
	Deliveries	Parts or tooling delivery				Y
Decommissioning	Decommissioning Survey	As Geophysical surveys		Y		
	Support Structure Decommissioning	Assessment and removal of foundation structure	Y		Y	
	Cable Decommissioning	Remove cable from sea floor	Y		Y	
	Life extension/repowering surveys	Cable, support structure surveys	Y		Y	
Full lifecycle	Emergency response	Search		Y		Y
		Recovery		Y		Y
	Security	Patrols				Y

### 3.5 Understanding of Autonomous Systems in the Offshore Wind Industry

It is clear that autonomous systems can have a future in the offshore wind industry. However, there is sometimes a disconnect in understanding between the autonomous system technology developers and offshore wind developers or owner-operators. To ensure the autonomous system being designed is appropriate for use, it is imperative that technology developers understand the processes and risks associated with operating around offshore wind farms. Similarly, for autonomous systems to be commercially accepted by wind farm developers and owner operators, the risks posed by the autonomous system to the offshore wind farm need to be understood and quantified. One specific area of concern is the cyber security ramifications of operating autonomous systems within or around wind farms. The remainder of this report will explore the cyber security risks associated with autonomous systems, with an initial focus on cyber security as a whole and best practice guidance.

## 4 CYBER SECURITY OVERVIEW

### 4.1 Relevant Standards and Regulations

There are a number of International, UK and European Union (EU) standards relating to cyber security as shown in Table 5. Whilst General Data Protection Regulation (GDPR) does not explicitly focus on cyber security, the requirement to protect data is inherently part of cyber security and therefore this has been included within the table below.

Table 5 Relevant standards and regulations for cyber security

Standard/Regulation	Description
ISO/IEC 27001	Information security, cyber security and privacy protection. Information security management system requirements.
PD ISO/IEC 27001:2022 - SME Handbook	Information Security Management Systems. A practical guide for SMEs.
BE EN IEC 62443	A collection of nine standards, technical reports and technical specifications each developed to secure industrial automation and control systems (IACS) throughout their lifecycle [29].
NIS2 Directive	The EU's framework for Cyber security across critical industries such as energy, health and banking [30].
GDPR	Legal requirement to protect the data of citizens by adopting privacy by design [31].
Cyber Assessment Framework	A systematic and comprehensive framework to assess how cyber risks to essential functions are being managed by the organisation responsible [32].

## 4.2 Best Practice

The National Cyber Security Centre (NCSC) provides advice and guidance on many elements of cyber security and is an excellent resource for companies of varying size, such as the 10 Steps to Cyber Security Guidance [33] (Figure 9) and Small Business Guide: Cyber Security [34].



Figure 9 NCSC 10 steps to Cyber Security infographic [35]

In addition to the steps set out by the NCSC, the common threads of good practice in Figure 10 were recommended during stakeholder engagement. These recommendations align with the standards and regulations mentioned in Table 5.

### Principle of least privilege

- Restricting the access of users and systems to the least amount possible while still being able to accomplish their tasks.

### Zero trust architecture

- A strategy assuming no user or device can be trusted and therefore it must be verified and authorised for each use.

### Memory safe hardware

- The use of memory safe hardware to mitigate against “memory safety vulnerabilities” in software. The ongoing Capability Hardware Enhanced RISC Instructions (CHERI) research project has developed hardware to mitigate these vulnerabilities and highlights the need for cyber security to be considered at the design stage.

### Manage vulnerabilities

- The continuous process of identifying, assessing and mitigating vulnerabilities to prevent cyber-attacks. Such as using vulnerability scanners to assess weaknesses and patch management software to, where appropriate, ensure software is up-to-date.

### Password management

- Using encrypted password managers to store and generate passwords, ensuring they are different for all applications and regularly changed.

### Multi-factor authentication

- Also known as 2-step verification or two-factor authentication, this requires the use of a password and another form of authentication, such as a unique code sent to a mobile number or email address, a fingerprint scan or authentication app.

### Firewalls

- Hardware and software firewalls act as barriers to block cyber-attacks.

### Multi-layered security approach/Defence-in-depth

- Using multiple barriers across different layers to reduce the likelihood of an attack reaching critical systems. According to IBM the layers from system level, through to network level, application level and transmission level should all be protected [9].

### Monitor global threats and attacks

- By monitoring global attacks system patches and security measures can be implemented as soon as possible, reducing the likelihood of susceptibility to these attacks.

### Network segregation

- Using virtual local area networks (VLANs) or hardwired segregation to divide the network into isolated segments. While VLANs are appropriate in many organisations, hardwired segregation is likely to be required around critical national infrastructure.

### Data Encryption/Cryptography

- The process of transforming data into an unreadable format using an encryption key, rendering it useless if intercepted/stolen.

### Cyber incident response planning

- Having a plan in place to ensure an attack can be contained and damage minimised.

Figure 10 Cyber security good practice

#### 4.2.1 The CIA Triad of Information Security

The CIA Triad (shown in Figure 11) is a model that has been used in information security since the 1970s. The three principles set out (Confidentiality, Integrity and Availability) are crucial in maintaining the security of an organisation and work together to guide organisational procedures and policies. ISO/IEC 27001 and the NIST Cybersecurity Framework have adopted these principles to ensure data protection.

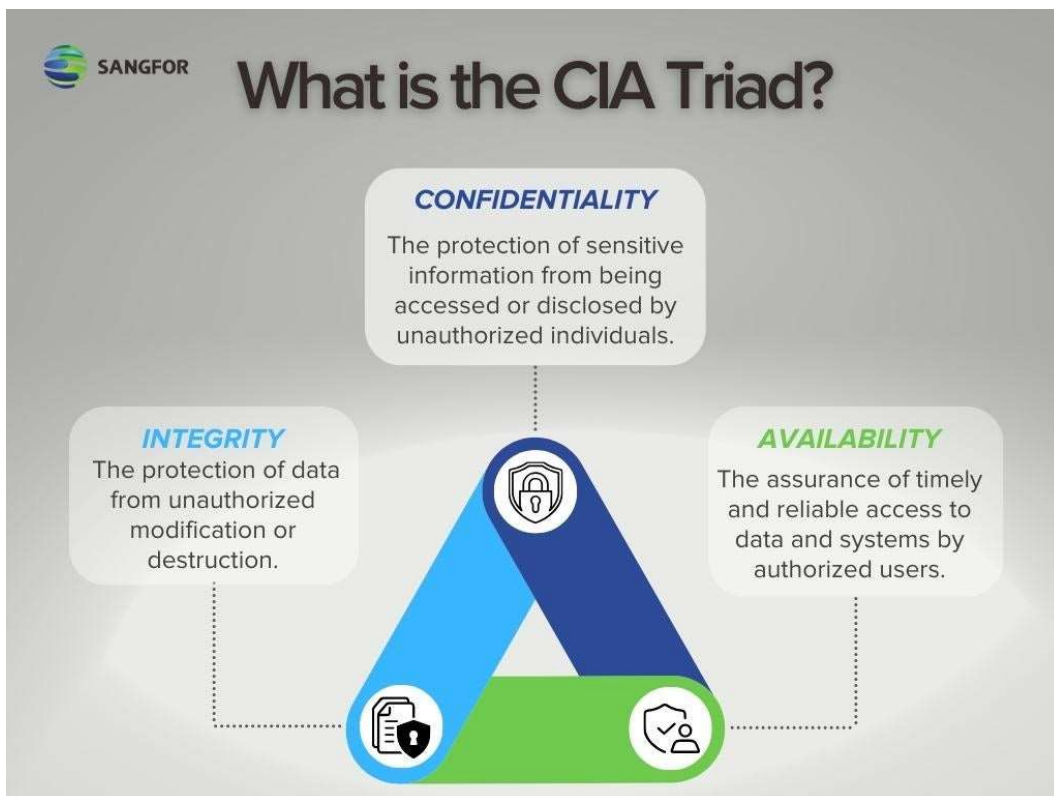


Figure 11 The CIA triad [36]

In addition to confidentiality, integrity and availability, authenticity and non-repudiation can also be considered as key principles:

- **Authenticity:** Ensuring that the information or data is true and correct by putting in place access control measures. Ensuring those accessing data are who they say they are through user authentication methods.
- **Non-repudiation:** Ensuring methods are put in place to prove actions have been completed. Ensuring data is delivered correctly with the sender and receiver of information able to validate the sending and receiving.

#### 4.2.2 Certification Schemes

Individual and company certification schemes may be useful to prove competency and adherence to best practice. Resources such as the UK Cyber Security Council certification framework [37] and CyberSmart [38] are useful to understand different certifications available.

In the UK the government-backed Cyber Essentials certification scheme offers two levels of certification, Certified and Certified Plus. The National Cyber Security Centre (NCSC) recommends this as the minimum standard for all organisations, offering support and advice to help organisations achieve certification [39]. There is also an EU Cyber Certification scheme which aims to provide evidence of compliance with regulatory requirements [40].

Although not a certification scheme, the NCSC Cyber Assessment Framework [32] is a tool for assessing and demonstrating the cyber resilience of an organisation across four high-level objectives:

1. Managing security risk
2. Protecting against cyber-attack
3. Detecting cyber security events
4. Minimising the impacts of incidents

Assessments can be completed by the organisation itself (self-assessment) or an independent cyber resilience auditor [41].

#### 4.2.3 Detecting and Managing Vulnerabilities

Detecting and managing vulnerabilities is one of the 10 steps to Cyber security (Figure 9). A proactive process that could be followed to manage vulnerabilities is shown in Figure 12. In the detect stage the following methods could be used [42]:

- Vulnerability scanning
- Penetration testing
- Patch management
- File integrity monitoring
- Continuous network monitoring



Figure 12 Vulnerability management process [43].

### 4.3 Attack Types

There are multiple types of attacks that are detailed across various resources - a selection of these is listed below. It should be noted the effects of an attack may go unnoticed for long periods of time if the attackers choose not to act immediately.







Table 6 Attack Types [44], [45], [46]

Attack type	Description
Blanket/Un-targeted	Attackers target as many devices, users or services as possible, without discrimination. They may scan the internet for weaknesses or send phishing emails to large numbers of addresses.
Targeted	Attackers single out an organisation for attack. There could be many reasons, and one technology developer cited an increase in attacks around their publicity events. Attackers may send spear-phishing emails to target individuals, or attack equipment or software in the supply chain that will be delivered to the organisation.
Ransomware	When ransomware is downloaded, it encrypts the user's workstation or the server to prevent access. The ransomware could be downloaded from a website, email or USB. The attacker may demand payment to unlock the system.
Malware	Malicious software is downloaded to exploit the users' devices. Some common types include: a rootkit which opens a backdoor to the device; a trojan horse that appears harmless but executes malicious code; or spyware that monitors the user's activity, login credentials and sensitive information.
Internal/Insider	Insiders or internal personnel could use their normal access to launch an attack or encourage colleagues to break security practices, enabling them to access information beyond their normal clearance (refer to the principal of least privilege). Perhaps a disgruntled employee or someone working for an adversary, they would be able to damage and steal data or create back doors for further attacks.
Man-in-the-middle (MITM)	MITM attacks are those where an attacker positions themselves between two communicating parties and is able to eavesdrop on any data or information sent between them.
Denial-of-service (DoS) and distributed-denial-of-service (DDoS)	DoS attacks are where the attacker makes the service or system unusable by overwhelming it and therefore preventing its ability to perform normal operations. In DDoS attacks the aim is the same but across multiple areas.

### 4.3.1 Attack Motivations

Whilst it is not the purpose of this report to understand why a cyber-attack may be undertaken, it should be recognised there are different categories of attacker, not all of whom have malicious intent.

Table 7 Types of attackers and their motivations [47].

Hat colour		Hat description
	Black hat hackers	Also known as malicious hackers, they use their technical skills to gain money by defrauding or blackmailing. They break into the system without permission by exploiting vulnerabilities and bypassing security protocols.
	White hat hackers	Also known as ethical hackers, they use their technical skills to protect against other hackers and operate within a legal framework. They may be motivated to find and fix vulnerabilities, improve software security and develop tools to detect cyber-attacks.
	Grey hat hackers	Similar to white hat hackers, grey hat hackers often have good intentions. However, they may choose to operate outside the legal framework such as by looking for vulnerabilities without consent. Grey hat hackers often draw the owner's attention to their vulnerabilities, but may also release these publicly, which may damage reputation or open up the company to further attacks.
	Red hat hackers	Also known as vigilante hackers, they seek to rid the world of black hat hackers, often using illegal and extreme routes to do so.
	Blue hat hackers	There are two types of blue hat hackers: <ol style="list-style-type: none"> <li>1. Also known as vengeful hackers, they are out to take personal revenge, such as a disgruntled employee against their employer.</li> <li>2. External security professionals invited in to test new software and find the vulnerabilities before it is released</li> </ol>
	Green hat hackers	Also known as unskilled hackers, they are often unaware of the consequences of their actions and cause unintentional damage.

### 4.4 Detecting an Attack

According to the Mandiant M-Trends 2024 report [48] the median dwell time to detect a successful attack globally in 2023 was 10 days. However, across the regions of Europe, the Middle East and Africa (EMEA) this increased to 22 days, with 56% of attacks detected within 30 days and 89% within 6 months. Figure 13 shows these timescales in comparison with the global trend, with Japan and Asia Pacific (JAPAC) and with the Americas, emphasising that EMEA is lagging behind the global trends for detection. The increased dwell time in EMEA appears to be due to an increase in non-ransomware attacks going undetected by companies for longer periods of time. However, research suggests it is not the time to detection that affects the severity of an attack but rather the type of attack and attacker [49].

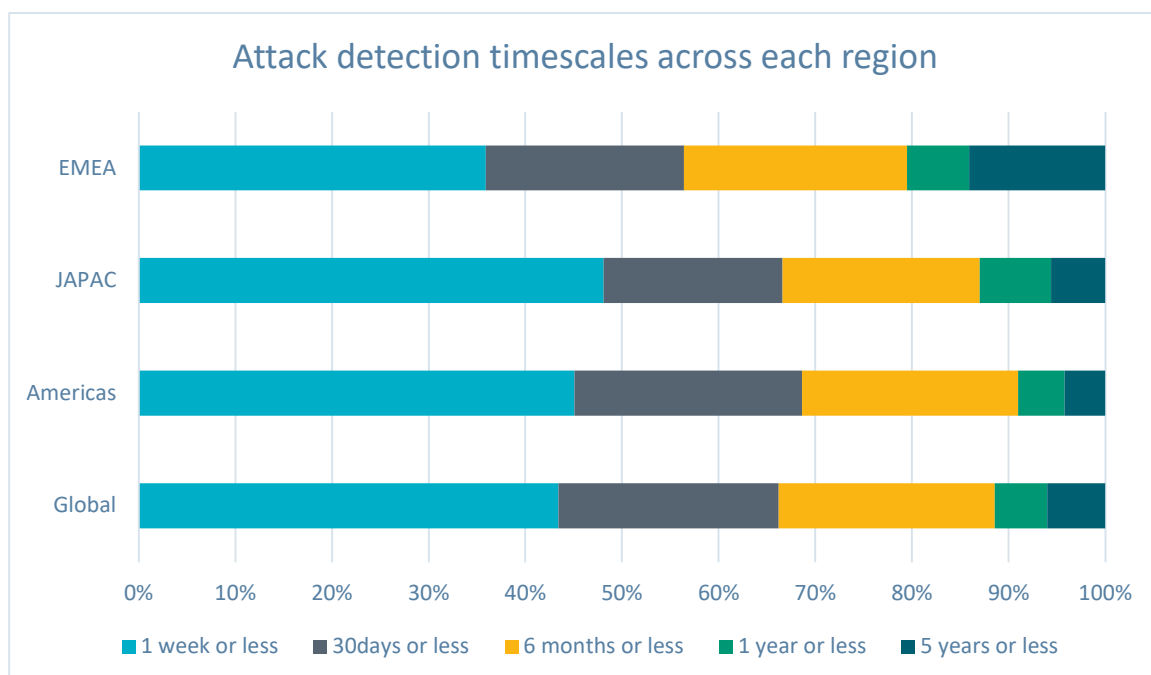


Figure 13 Attack detection timescales across each region

There are various methodologies and software applications to assist in detecting attacks. One such methodology is to install a condition monitoring system on the network during the construction phase of a project which could:

- Monitor the location of attackers/those trying to login to the network.
- Monitor traffic flow.
- See failed authentication requests.
- Flag unusual activity, such as repeated log ins and repeated or unexpected instructions.

An additional methodology is to use endpoint detection and response tools to detect malicious activity and threats at endpoints such as laptops. Furthermore, as artificial intelligence (AI) and machine learning (ML) capabilities improve these may be used to detect anomalies and attacks.

## 5 CYBER SECURITY AND AUTONOMOUS SYSTEMS

### 5.1 Relevant Standards, Regulations and Guidance

In addition to the general cyber security standards shown in Table 5, a non-exhaustive list of other standards relevant to the cyber security of autonomous systems is shown in Table 8.

Table 8 Relevant standards and regulations for the cyber security of autonomous systems

Standard/Regulation/Guidance	Description
BS EN IEC 63154:2021	Maritime navigation and radiocommunication equipment and systems. Cyber security. General requirements, methods of testing and required test results.
CAP 2973	UK Civil Aviation Authority (CAA): Cyber security guidance for innovators.
NR 659 RO4	BV: Rules on Cyber Security for the Classification of Marine Units
UR E26	International Association of Classification Societies (IACS): Cyber resilience of ships.
UR E27	IACS: Cyber resilience of on-board systems and equipment.
Workboat Code Edition 3	Maritime & Coastguard Agency (MCA): The Safety of Small Workboats and Pilot Boats – A Code of Practice

#### 5.1.1 BS EN IEC 63154:2021

This standard addresses the basic cyber security requirements for ship navigation and radio communication equipment on vessels subject to the Safety of Life at Sea (SOLAS) Convention.

#### 5.1.2 CAP 2973: Cyber security guidance for innovators

A general introduction to cyber security in the aviation industry. The guide provides information and links to further relevant regulations and publications in section 3 and support for the development of cyber security risk assessments outlined in section 4.

#### 5.1.3 NR659 RO4: Rules on cyber security for the classification of marine units

Specifically applicable to computer-based systems (CBS) that rely on software for their functionality on classified ships. This rule note applies to USVs since they form part of the classifications in NR467 A R23: Part A – Classification and Surveys.

#### 5.1.4 UR E26 and UR E27

Focusing on the cyber resilience of on-board systems and ships as a whole, these unified requirements are applicable to ships and vessels as described in Table 9.

Table 9 UR E26 and UR E27 scope of applicability [50], [51]

Mandatory requirements for:	Non-mandatory guidance to:
<ul style="list-style-type: none"> <li>• Passenger ships (including passenger high-speed craft) engaged in international voyages</li> <li>• Cargo ships of 500 GT and upwards engaged in international voyages</li> <li>• High speed craft of 500 GT and upwards engaged in international voyages</li> <li>• Mobile offshore drilling units of 500 GT and upwards</li> <li>• Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation)</li> </ul>	<ul style="list-style-type: none"> <li>• Ships of war and troopships</li> <li>• Cargo ships less than 500 GT</li> <li>• Vessels not propelled by mechanical means</li> <li>• Wooden ships of primitive build</li> <li>• Passenger yachts (passengers not more than 12)</li> <li>• Pleasure yachts not engaged in trade</li> <li>• Fishing vessels</li> <li>• Site specific offshore installations (i.e. Floating Storage Units and Floating production, storage and offloading vessels)</li> </ul>

### 5.1.5 Workboat Code Edition 3

Specific to surface vessels <24 m that are operated by a crew or remote operation centre. Excludes underwater and/or autonomous vessels, although some of the principles are useful to consider in these areas. Section 31 and Annex 2 Section 8 give specific information on cyber security.

## 5.2 Cyber Security and Autonomous Systems Best Practice

Best practice for cyber security and autonomous systems operating in and around offshore wind farms (OWFs) can be broadly split into five categories (Figure 14). These should be considered in line with best practices for cyber security in general.

One additional area to consider is that technology development moves at a quick pace and cyber security developments have come a long way. However, on the social side a shift is needed in human thinking and understanding. As such, cultural change can appear to move at a comparatively glacial pace. Therefore, within most systems it is often the end user that is the weakest link and out of the control of technology providers.

Furthermore, it is imperative to ensure systems have fail-safes and redundancies. For example, if there is a loss of communication with the satellite navigation system then performing a predefined holding pattern could be a safe solution until systems are operational again.

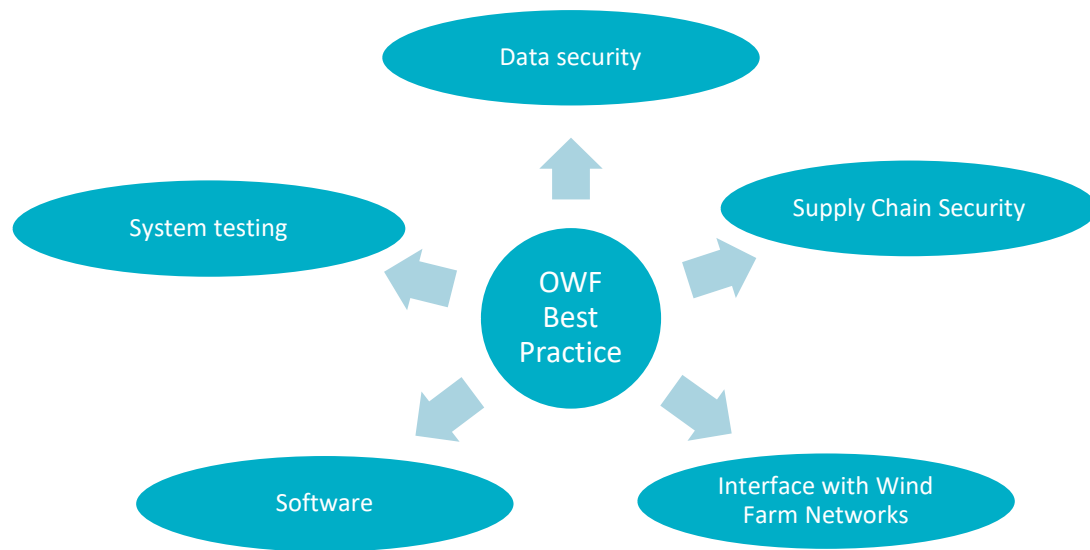


Figure 14 Best Practice categories of Cyber Security and Autonomous Systems

### 5.2.1 Data Security

Data is most vulnerable during data transfer. This can be between: ROC and vessel; vessel and cloud; or vessel and vessel. However, data is also at risk whilst being stored. Data can be protected by:

- Using data encryption.
- Uploading data to the cloud at specific times and as quickly as possible to ensure the network is not open for long.
  - Only open the network for data transfer when the data is ready.
  - Check sensor settings so they only transfer when instructed to do so – some sensors are set to upload whenever they find an internet connection which may leave them susceptible to attack.
- Protecting cloud storage with rotating encryption keys.
- Giving different users appropriate levels of access.
- The integrity of satellite communications and navigations systems if using these.

### 5.2.2 Supply Chain Security

Multiple suppliers can be involved in the development of a single system. This poses risks to the user of the final product. Measures should be put in place to ensure the integrity of the system:

- Complete a cyber security test of the full system.

- Use an appropriate company quality management system (QMS) to ensure reputable suppliers are used and all appropriate processes are followed throughout the design stage and into deployment.
- Ensure supply chain procedures are robust and reputable suppliers are used.
- Where appropriate, check the cyber security certification of all parties in the supply chain.

### 5.2.3 System Testing

The aim of testing is to prove the system does what you want it to, and never does what you don't want it to. This could include penetration testing or thorough test programmes through facilities such as the Cyber-SHIP Lab at the University of Plymouth [52]. Testing could be full system or partial system testing. In either case it should be clear what was tested and what the results were.

### 5.2.4 Interface with Wind Farm Networks

Where network access is required, ideally the system would use the following in preferential order:

1. Satellite
2. 5G network
3. Wind turbine generator (WTG) Wi-Fi (where appropriate)
4. OWF Network – Ancillary or similar (if available)
5. OWF Network - Control

Satellite communication systems such as Starlink and Iridium may be used for communication. The use of these systems requires no interaction with the wind farm network and as such the autonomous system is kept completely separate. The cyber security of satellite systems is dependent on, and the responsibility of, the satellite owners; however, the autonomous system developer holds responsibility for which satellite system they choose.

Most satellite navigation systems use GNSS, which encompasses systems such as GPS, GLONASS, Galileo and BeiDou. Each system has its own weaknesses and the spoofing and jamming of satellite navigation systems is thought to be common, therefore this should be taken into consideration in the design of autonomous systems.

Most OWFs currently under installation or planned in the future are likely to have a private 5G network installed to cover the OWF site. Unlike public 5G networks, a private 5G network is under complete control of the OWF developer or owner operator and any downtime/work required will be controlled by them. These networks are typically designed for high availability and resilience; however, they remain subject to environmental and electromagnetic influences. For example, large vessels such as cruise ships passing in proximity to the OWF may introduce radio frequency (RF) interference, contribute to spectrum congestion (particularly in shared spectrum bands), or cause signal attenuation due to physical obstruction. Such factors can temporarily impact the performance of the private 5G network, including latency, throughput, or reliability

Every OWF will have a hardwired network set up for communication with the SCADA that will run from each WTG back to the onshore control room. OWFs installed post-2023 are expected to have

multiple networks to enable the segregation of systems. The number of networks installed can vary - one possible model is four networks for control, non-control, high voltage and ancillary purposes. In this scenario the ancillary network is most likely to be suitable for access by autonomous systems if required. As the ancillary network is physically disconnected from the control and other networks these could not be compromised in the event of a successful cyber-attack.

Where access to any control information or data is critical to the autonomous system this should be carefully considered. It may be possible to link the system into the control network, but extra precautions should be agreed and a cyber risk assessment undertaken.

OWFs installed pre-2023 are more likely to have a single network. Whilst it may be possible to increase the number of networks to enable physical distinction between the control and ancillary systems, this would need to be investigated. It may be possible to create a VLAN network in this scenario, however this should be treated with caution.

### **5.2.5 Software**

Open-source software is widely used. One risk of this is that a hacker could create their own open-source software and others could use this. It is thought to be unrealistic to test every piece of software used. An additional risk is the availability of the source code in open-source software, making it easier for hackers to identify and exploit vulnerabilities, although the open nature of the code means that software can be assessed for the level of threat it poses based on whether vulnerable components are used by the application. Where possible, formal methods is one approach that could be used to certify software and provide confidence, however this does not negate the risk of the source code being openly available.

## **5.3 Cyber Security Risks**

The risks associated with an ASV/AUV are perceived to be similar to those of an USV. Similarly, the risks associated with an autonomous ROV and drone are perceived to be similar to that of an ROV and UAV. Therefore, it could be interpreted that many of the risks associated with autonomous systems are already implied as accepted through the current use of USVs, ROVs and UAVs. The following section highlights some of the perceived cyber security risks (Table 10), factors affecting risks (Table 11) and possible mitigations (Table 12) for operating autonomous systems in and around OWFs.

### 5.3.1 Perceived Cyber Security Risks

Table 10 Perceived cyber security risks

Risk	Description
GNSS spoofing/jamming	<p>GNSS is very susceptible as it has a weak signal.</p> <p>Jamming is the deliberate interference of a signal, preventing it from reaching the receiver.</p> <p>Spoofing is the transmission of false signals to the receiver.</p>
Collision	Possible collisions include collisions with infrastructure and other vessels or aircraft.
Entanglement	Navigating around tethers, cables or moorings will be challenging.
Shipping lanes	Entering ship navigation lanes during transit which may result in collision with large ships.
Command loop hacked/intercepted communications	<p>Spurious movements or actions as a result.</p> <p>Loss of vessel or aircraft if sent to an unknown location.</p>
Data harvesting	Intercepting and stealing data. Data stolen now could be used for nefarious activities at a later date. For example, intercepting data on the location of an export cable between an offshore wind farm and the onshore substation now that may enable an attack on the cable in five years' time.
Data manipulation	Changing results or adding erroneous results to data which may lead to erratic behaviour of vessels or aircraft. It could also result in this data being used for other purposes by the client, thus threatening the integrity of these processes.
WTG control system access	Access to the WTG SCADA system could enable settings to be changed that lead to turbine damage and possible risk to human life.
Multiple suppliers integrated into one autonomous system	Ensuring the full system is secure when multiple suppliers are involved is a challenge. It would be possible for a supplier to leave a back door open into the system that enables access at a later date. For example, the German Institute for Defense and Strategic Studies has issued a report stating the use of Chinese manufacturers on wind farms leaves a door open for the delay in wind farm operation, harvesting of sensitive data and remote shut down of turbines due to the political climate [53].
Vessel 'fuel' system	The contents of a vessel may have its own inherent risk that has implications for vessel collision. For example, a diesel-powered vessel has a different risk profile to one powered by hydrogen fuel cells.
Sensor capability	Internet of Things (IoT) sensors are only capable of very basic security and encryption methods. Therefore, they are vulnerable to attack.

### 5.3.2 Factors Affecting Cyber Security Risks

Table 11 Factors affecting cyber security risks

Factor affecting risk	Description
Inshore greater than offshore	If a vessel has a collision or sinks inshore it is more likely to create a hazard for other users due to the shallower water depths and increased number of vessels and people. In addition, a recovery operation is likely to be required resulting in otherwise unnecessary and potentially hazardous activities taking place.
Smaller vessels less of a concern than larger ones	Smaller vessels are likely to cause less damage than larger ones.
Hull material	The hull material will affect the likelihood and severity of damage. For example, the composite material used in the hull of the XO-450 by XOcean is likely to result in more damage to itself than other vessels or structures if a collision was to occur.
Number of vessels and aircraft	An increase in the number of vessels and aircraft operating in the area will likely result in an increased likelihood of collision.
Type and number of turbines	<p>Fixed turbines have a much lower risk of entanglement than floating turbines due to the absence of dynamic cables, mooring lines and potential turbine movement. Other risks of entanglement such as fishing nets or simultaneous operations using tethered ROVs are synonymous with fixed and floating wind farms.</p> <p>Newer turbines are larger in size and rating, therefore requiring more space between them and fewer turbines to be installed for the overall wind farm capacity. Therefore, navigation will likely be easier resulting in a reduced likelihood of collision.</p>
Operational speed	The operational speed of the vessel or aircraft will directly affect the severity of damage. For example, the maximum operational speed of XOcean’s XO-450 is 4 knots and therefore unlikely to do any harm [54].
Relationships with local fishermen	Wind farms located in areas popular with fishermen may have better support where there are positive relationships. Popular fishing areas will also result in an increased number of vessels and gear such as lobster pots in the area.
Wind farm location	The wind farm may be located in an area where spoofing and jamming of GNSS is widely used and therefore other mechanisms of navigation will be required. Certain locations are also more susceptible to piracy.
Software type used	The level of overall software verification and certification can provide confidence that the software is safe from a cyber security perspective.
Required interaction level with OWF network	Most autonomous systems will be independent of the SCADA and therefore the risk is low. However, any system requiring interaction with the SCADA will need careful planning and consideration.
Number of suppliers in the supply chain	The number of different supplier parts or manufacturers in the system and levels of confidence or testing for each supplier will affect the level of risk, as will full system testing.

Factor affecting risk	Description
Data transfer methodologies	<p>Data can be transferred live, periodically when connected to a network, or when docked at a docking station or inshore. These methodologies have a decreasing level of risk, although not all are appropriate for every task.</p> <p>The encryption of data during transfer will also decrease the risk, whereby if data is harvested it cannot be deciphered.</p>

## 5.4 Cyber Security Risk Mitigations

Table 12 Cyber security risk mitigations

Mitigation	Description
Network segregation	<p>Limiting access to the turbine network and preferring the use of satellite or 5G networks instead.</p> <p>Using separate networks for different tasks, such as a control network for turbine control and ancillary network for systems outside of this that require access to the turbine.</p>
Contingency planning	<p>Ensuring a plan is in place in the event of:</p> <ul style="list-style-type: none"> <li>• A loss of communication with the ROC.</li> <li>• A loss of communication with the navigation system.</li> <li>• A suspected cyber-attack.</li> </ul> <p>This may include performing a holding pattern, sending a ‘ping’ of the last known address to the ROC, or having a standby vessel available to support.</p>
WTG isolation	<p>When work is being undertaken on a WTG it will be parked remotely, then the technicians gaining access will switch from remote to local control, removing the ability of the SCADA to restart the turbine. Depending on the work being undertaken there may also be other system isolations which can prevent the turbine from being operated remotely whilst technicians are accessing the turbine.</p>
Limited autonomy	<p>Putting guardrails in place until confidence is built up in the system. For example, allowing limited autonomy so the system can only take certain actions.</p>
Testing	<p>The testing of software using formal methods.</p> <p>The testing of partial and full systems prior to operation.</p>
Additional technologies	<p>Using additional technologies to mitigate against known issues, such as the unreliability of GNSS signal. For example, Sonardyne’s Sprint-Nav sensor has been developed to combat this issue [55]</p>
Multi-layered security approach	<p>Multiple firewalls used so that if the first layer is broken into further steps are needed to access the most critical systems.</p>

## 6 CONCLUSION

---

Given the expected growth of the offshore wind industry, the use case for RAS is undeniable. There is growing confidence in the use of remotely operated systems such as UAVs, USVs and ROVs, however these are all currently human-in-the-loop operations. As the confidence in technology grows there will likely be a step forward in the degree of autonomy towards systems being supervised by humans and ultimately becoming fully autonomous. Improved regulation will be needed before the full commercial opportunity of this can be realised.

The cyber security risks of autonomous systems are high in certain areas, but not much greater than the remotely operated systems currently in use. To mitigate the risk of attacks occurring, it is critical that the principles of best practice are followed. In addition, the toolkit [1] can be used to provide questions and highlight further mitigations to reduce the risk profile of certain systems and provide decision-makers with the confidence required for technology adoption.

## 7 RECOMMENDATIONS

---

### 7.1 Technology Developers

The following recommendations are made to technology developers:

- Consider the cyber security of the system from the initial design stages, following the principle of 'Secure by Design' set out in the Cyber Assessment Framework [32].
- Factor in supply chain cyber security requirements and ensure robust supply chain procedures are used.
- Consider applying for a cyber security certification scheme to build confidence in your business.
- Perform cyber security testing on the system where possible.
- Ensure fail-safes and contingencies are integrated into the system in case of emergency.
- Complete a cyber security risk assessment for the autonomous system to share with decision-makers.
- Recognise the use of autonomous systems in OWFs is a new concept and therefore the industry will likely be nervous to introduce them. Address their concerns by providing technology demonstrations in a controlled environment, such as at a testing & assurance centre.
- Use the toolkit to understand some of the questions decision-makers might want to ask.

### 7.2 Decision-Makers

The following recommendations are made to decision-makers who control the adoption of autonomous technologies:

- Complete a cyber risk assessment, understanding the key risk areas in the OWF prior to autonomous systems becoming common place. Understand factors such as the number of

networks available, turbine lock-off mechanisms and areas with weak satellite navigation systems.

- Be open-minded and work collaboratively with technology developers to identify any specific areas of concern and opportunities for development.
- Use the toolkit to support with identifying questions to ask and what the specific risks may be given the considerations of the OWF.
- Recognise the cyber security risks associated with autonomous systems are not dissimilar to those posed by USVs, ROVs and UAVs already in operation across the industry.

### 7.3 Future Priority Areas

The following areas have been identified as future priorities:

- The development and understanding of regulations across all vehicle types (surface, subsurface and aerial). It should be recognised that where no regulation currently exists, and when technology is not fully understood there can be a tendency to over-regulate which may be as obstructive as a lack of regulation. The coordination of international regulators would be advantageous to develop appropriate regulations regardless of geographical location.
- The training of personnel involved within offshore wind with regard to cyber security best practices and the use of autonomous systems within wind farms.
- The enabling of improved access to system testing so that technology developers can develop cyber-resilient systems.
- A desktop study of cyber security frameworks and best practices across other industries, such as aviation, nuclear and automotive, to inform the cyber security related decisions made in the offshore wind industry.

## 8 REFERENCES

---

- [1] R. Wilson-Nash, “PN000844-DOC-007\_Cyber Security and Autonomous Systems Toolkit,” Offshore Renewable Energy Catapult, Glasgow, 2025.
- [2] Net Zero Technology Centre, “Offshore Low Touch Energy Robotics & Autonomous Systems,” Net Zero Technology Centre, 2023. [Online]. Available: <https://olter.co.uk/>. [Accessed 13 March 2025].
- [3] L. Forbes and J. Jermier, “Workplace Autonomy,” in *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, Amsterdam, Elsevier, 2015, pp. 718-721.
- [4] D. Mitchell, J. Blanche, S. Harper, T. Lim, R. Gupta, O. Zaki, W. Tang, V. Robu, S. Watson and D. Flynn, “A review: Challenges and opportunities for artificial intelligence and robotics in the offshore wind sector,” *Energy and AI*, vol. 8, p. 100146, 2022.
- [5] International Maritime Organization, “Autonomous Shipping,” n.d.. [Online]. Available: <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx>.
- [6] H. Sivori and L. Brunton, “Out of the box – Implementing autonomy and assuring AI in the maritime industry,” 26 April 2023. [Online]. Available: [https://maritime.lr.org/l/941163/2023-04-17/75wsr/941163/1682383431twVrCNID/Thetius\\_LR\\_\\_\\_Out\\_of\\_the\\_box\\_\\_\\_Autonomy\\_and\\_AI\\_2023.pdf](https://maritime.lr.org/l/941163/2023-04-17/75wsr/941163/1682383431twVrCNID/Thetius_LR___Out_of_the_box___Autonomy_and_AI_2023.pdf). [Accessed 5 March 2025].
- [7] Bureau Veritas, “Autonomous ships,” Bureau Veritas, n.d.. [Online]. Available: <https://marine-offshore.bureauveritas.com/marine/autonomous-ships>. [Accessed 5 March 2025].
- [8] Bureau Veritas, “NI641 R01 : Guidelines for Autonomous Shipping,” Bureau Veritas, Paris, 2019.
- [9] AS Mosley, “Digital Twin for Floating Offshore Wind Turbines,” AS Mosley & Co Ltd, n.d.. [Online]. Available: <https://xocean.com/>. [Accessed 2 April 2025].
- [10] ADVANCED NAVIGATION, “What is the definition of UAV?,” ADVANCED NAVIGATION, 2025. [Online]. Available: <https://www.advancednavigation.com/glossary/uav/>. [Accessed 2 April 2025].
- [11] XOCEAN, “Homepage,” XOCEAN, n.d.. [Online]. Available: <https://xocean.com/>. [Accessed 2 April 2025].
- [12] Geo-matching, “GAVIA Osprey AUV,” Geo-matching, 2025. [Online]. Available: <https://geo-matching.com/products/osprey-auv>. [Accessed 2 April 2025].
- [13] National Marine Sanctuary Foundation, “What is an ROV?,” National Marine Sanctuary Foundation, 27 April 2020. [Online]. Available: <https://marinesanctuary.org/blog/what-is-an-rov/>. [Accessed 2 April 2025].
- [14] S. Fawcett and T. Fileman, “ACORD Autonomous Platforms Audit: Final Report,” PML Applications, Plymouth, 2024.

- [15] Robotics Growth Partnership, “Smart Machines 2035: A Strategy for UK Leadership,” Department for Science, Innovation and Technology, London, 2025.
- [16] UK Civil Aviation Authority, “New trials set to help unlock drone deliveries and inspections in the UK,” UK Civil Aviation Authority, 15 August 2024. [Online]. Available: <https://www.caa.co.uk/newsroom/news/new-trials-set-to-help-unlock-drone-deliveries-and-inspections-in-the-uk/>. [Accessed 15 April 2025].
- [17] Maritime and Coastguard Agency, “The Workboat Code Edition 3,” 22 January 2025. [Online]. Available: <https://www.gov.uk/government/publications/the-workboat-code-edition-3>. [Accessed 2 April 2025].
- [18] Maritime and Coastguard Agency, “MGN 702 (M) Amendment 1 Maritime autonomous surface ships of less than 2.5 metres in LOA,” 19 March 2025. [Online]. Available: <https://www.gov.uk/government/publications/mgn-702-m-amendment-1-maritime-autonomous-surface-ships-of-less-than-25-metres-in-loa>. [Accessed 2 April 2025].
- [19] Maritime and Coastguard Agency, “MGN 705 (M) Remotely operated unmanned vessels (ROUVs) of 2.5 metres to less than 4.5 metres in length overall,” 31 December 2024. [Online]. Available: <https://www.gov.uk/government/publications/mgn-705-m-remotely-operated-unmanned-vessels-rouvs-of-25-metres-to-less-than-45-metres-in-length-overall>. [Accessed 2 April 2025].
- [20] XOCEAN, “Technology,” XOCEAN, 2023. [Online]. Available: <https://xocean.com/technology/>. [Accessed 6 March 2025].
- [21] Fugro, “Fugro pioneers uncrewed subsea inspections in Brazil for Petrobras,” Fugro, 18 December 2024. [Online]. Available: <https://www.fugro.com/news/business-news/2024/fugro-pioneers-uncrewed-subsea-inspections-in-brazil-for-petrobras>. [Accessed 6 March 2025].
- [22] P. Vidan, M. Bukljaš, I. Pavić and S. Vukša, “Autonomous Systems & Ships -Training and Education on Maritime Faculties,” in *International Maritime Science Conference*, Budva, 2019.
- [23] Greensea IQ, “OPENSEA Edge Delivers Untethered Autonomous Operation to Commercially Available ROVs,” Greensea IQ, 22 March 2023. [Online]. Available: <https://greenseaiq.com/news/opensea-edge-delivers-untethered-autonomous-operation-to-commercially-available-rovs/>. [Accessed 6 March 2025].
- [24] National Oceanography Centre, “National Oceanography Centre (NOC) – Written evidence (AUV0056),” Parliament Committee, 2016 October 26. [Online]. Available: <https://committees.parliament.uk/writtenevidence/74298/html/#:~:text=3.1%20Yes%20%2D%20the%20current%20national,potentially%20not%20carry%20any%20insurance..> [Accessed 3 April 2025].
- [25] UK Marine Industries Alliance, “Industry Code of Conduct for Maritime Autonomous Systems,” 15 May 2018. [Online]. Available: <https://www.maritimeuk.org/media-centre/publications/industry-code-conduct-maritime-autonomous-systems/>. [Accessed 3 April 2025].

- [26] N. Skopljak, "Remotely Controlled Survey Wraps Up at Greater Gabbard," offshoreWIND.biz, 22 January 2020. [Online]. Available: <https://www.offshorewind.biz/2020/01/22/remotely-controlled-survey-wraps-up-at-greater-gabbard/>. [Accessed 20 March 2025].
- [27] A. Lee, "Unmanned offshore data harvesting in the North Sea," Sonardyne, 5 September 2019. [Online]. Available: <https://www.sonardyne.com/unmanned-offshore-data-harvesting-in-the-north-sea/>. [Accessed 20 March 2025].
- [28] M. Fisher, M. Webster, A. Loudon, H. MacDonald, J. van Stappen, J. Osnabrugge and D. Wavell, "Verifying Autonomy for Offshore Renewable Energy Applications," ORCA Hub, Edinburgh, 2022.
- [29] Editorial Team, "Understanding IEC 62443," 26 02 2021. [Online]. Available: <https://www.iec.ch/blog/understanding-iec-62443>.
- [30] Cyber Risk GmbH, "The NIS 2 Directive," Cyber Risk GmbH, 21 November 2024. [Online]. Available: [https://www.nis-2-directive.com/#:~:text=NIS%20%20\(Directive%20\(EU\),and%20resilience%20in%20their%20operations..](https://www.nis-2-directive.com/#:~:text=NIS%20%20(Directive%20(EU),and%20resilience%20in%20their%20operations..) [Accessed 13 March 2025].
- [31] Government Digital Services, "Meet the requirements of data privacy regulations," CROWN Copyright, 23 February 2024. [Online]. Available: [https://www.gov.uk/guidance/meet-the-requirements-of-data-privacy-regulations#:~:text=The%20General%20Data%20Protection%20Regulation%20\(GDPR\)%20came%20into%20force%20on,cannot%20align%20to%20the%20commitment..](https://www.gov.uk/guidance/meet-the-requirements-of-data-privacy-regulations#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR)%20came%20into%20force%20on,cannot%20align%20to%20the%20commitment..) [Accessed 13 March 2025].
- [32] National Cyber Security Centre, "Cyber Assessment Framework," National Cyber Security Centre, 18 April 2024. [Online]. Available: <https://www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-to-caf>. [Accessed 14 March 2025].
- [33] National Cyber Security Centre, "10 Steps to Cyber Security," National Cyber Security Centre, 11 May 2021. [Online]. Available: <https://www.ncsc.gov.uk/collection/10-steps>. [Accessed 14 March 2025].
- [34] National Cyber Security Centre, "Small Business Guide: Cyber Security," National Cyber Security Centre, 8 October 2020. [Online]. Available: <https://www.ncsc.gov.uk/collection/small-business-guide>. [Accessed 14 March 2025].
- [35] National Cyber Security Centre, "10 steps to cyber security infographic," 11 May 2021. [Online]. Available: <https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf>. [Accessed 14 March 2025].
- [36] Sangfor Technologies, "What is the CIA Triad?," Sangfor Technologies, 24 May 2024. [Online]. Available: <https://www.sangfor.com/glossary/cybersecurity/what-is-cia-triad>. [Accessed 7 March 2025].

- [37] UK Cyber Security Council, "Certification Framework," UK Cyber Security Council, 2025. [Online]. Available: <https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/certification-framework/>. [Accessed 12 March 2025].
- [38] CyberSmart, "A guide to cybersecurity certifications in the UK," CyberSmart, 2025. [Online]. Available: <https://cybersmart.co.uk/a-guide-to-cybersecurity-certifications-in-the-uk/>. [Accessed 12 March 2025].
- [39] National Cyber Security Centre, "Cyber Essentials," National Cyber Security Centre, n.d.. [Online]. Available: <https://www.ncsc.gov.uk/cyberessentials/overview>. [Accessed 13 March 2025].
- [40] ENISA, "About EU Cyber Certification," ENISA, n.d.. [Online]. Available: [https://certification.enisa.europa.eu/about-eu-cyber-certification\\_en](https://certification.enisa.europa.eu/about-eu-cyber-certification_en). [Accessed 13 March 2025].
- [41] National Cyber Security Centre, "Cyber Resilience Audit," National Cyber Security Centre, 2024. [Online]. Available: <https://www.ncsc.gov.uk/schemes/cyber-resilience-audit/introduction>. [Accessed 14 March 2025].
- [42] H. Chheda, "Understanding Cybersecurity Vulnerabilities And How They Put You At Risk," SPRINTO, 9 September 2024. [Online]. Available: <https://sprinto.com/blog/cyber-security-vulnerabilities/>. [Accessed 18 March 2025].
- [43] H. Chheda, "Why Vulnerability Management Matters:The Silent Threats That Lurk In Your System:," SPRINTO, 2 December 2024. [Online]. Available: <https://sprinto.com/blog/vulnerability-management/>. [Accessed 18 March 2025].
- [44] National Cyber Security Centre, "Common cyber attacks: reducing the impact," June 2016. [Online]. Available: <https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact>. [Accessed 6 March 2025].
- [45] Fortinet, "Types Of Cyber Attacks," Fortinet, n.d.. [Online]. Available: <https://www.fortinet.com/uk/resources/cyberglossary/types-of-cyber-attacks>. [Accessed 6 March 2025].
- [46] M. Cobb, "16 common types of cyberattacks and how to prevent them," TechTarget, 5 July 2024. [Online]. Available: <https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them#:~:text=Research%20and%20publishing%20firm%20Cybersecurity,try%20to%20protect%20enterprise%20resources..> [Accessed 6 March 2025].
- [47] M. Mehta, "Different Types of Hackers: The 6 Hats Explained," InfoSec Insights, December 10 2020. [Online]. Available: <https://sectigostore.com/blog/different-types-of-hackers-hats-explained/>. [Accessed March 6 2025].
- [48] Google Cloud Security, "Special Report: Mandiant M-Trends 2024," Google Cloud Security, 2025.
- [49] Y. Roumani and M. Alraee, "Examining the factors that impact the severity of cyberattacks on critical infrastructures," *Computers & Security*, vol. 148, p. 104074, 2025.

- [50] IACS, “UR E26 REV1: Cyber Resilience in Ships,” IACS, London, 2023.
- [51] IACS, “UR E27 REV1: Cyber resilience of on-board systems and equipment,” IACS, London, 2023.
- [52] University of Plymouth, “Cyber-SHIP lab,” University of Plymouth, n.d.. [Online]. Available: <https://www.plymouth.ac.uk/research/cyber-ship-lab>. [Accessed 20 March 2025].
- [53] V. Jack, “China could blackmail Germany via wind turbines, report warns,” Politico, 3 March 2025. [Online]. Available: <https://www.politico.eu/article/china-could-blackmail-germany-via-wind-turbines-government-linked-report-warns/>. [Accessed 21 March 2025].
- [54] XOcean, “XO-450,” XOcean, Co. Louth, n.d..
- [55] Sonardyne, “Dude, where’s my ocean robot?,” Sonardyne, 26 November 2024. [Online]. Available: <https://www.sonardyne.com/case-study/dude-wheres-my-ocean-robot/>. [Accessed 21 March 2025].
- [56] Cyber Essentials, “Welcome to the Cyber Essentials Knowledge Hub,” Cyber Essentials, 6 March 2025. [Online]. Available: <https://ce-knowledge-hub.iasme.co.uk/space/CEKH/2563768341/Welcome+to+the+Cyber+Essentials+Knowledge+Hub>. [Accessed 6 March 2025].
- [57] IBM, “The layered defense approach to security,” IBM, 7 October 2024. [Online]. Available: [https://www.ibm.com/docs/en/i/7.5?topic=ssw\\_ibm\\_i\\_75/rzaj4/rzaj40a0internetsecurity.html](https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/rzaj4/rzaj40a0internetsecurity.html). [Accessed 18 March 2025].
- [58] International Air Transport Association, “IATA Annual Security Report: 2023 Edition,” International Air Transport Association, 2024.
- [59] Mobileye, “A Brief History of Autonomous Vehicles – from Renaissance to Reality,” Mobileye, 27 February 2023. [Online]. Available: <https://www.mobileye.com/blog/history-autonomous-vehicles-renaissance-to-reality/>. [Accessed 21 March 2025].
- [60] Department for Transport, “Self-driving vehicles set to be on roads by 2026 as Automated Vehicles Act becomes law,” UK Government, 20 May 2024. [Online]. Available: <https://www.gov.uk/government/news/self-driving-vehicles-set-to-be-on-roads-by-2026-as-automated-vehicles-act-becomes-law>. [Accessed 21 March 2025].
- [61] Centre for Connected and Autonomous Vehicles, “The key principles of vehicle cyber security for connected and automated vehicles,” UK Government, 6 August 2017. [Online]. Available: <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles#downloadable-pdf-version>. [Accessed 21 March 2025].

## APPENDIX 1 LIST OF USEFUL RESOURCES

Title	Publisher	Year
<a href="#">NEW EU REGULATIONS - Whitepaper</a>	DNV	2025
<a href="#">CAP 2973: Cyber security guidance for innovators</a>	UK CAA	2024
<a href="#">NR 659 RO4: Rules on Cyber Security for the Classification of Marine Units</a>	BV	2024
<a href="#">UR E26: Cyber resilience of ships</a>	IACS	2023
<a href="#">UR E27: Cyber resilience of on-board systems and equipment</a>	IACS	2023
<a href="#">Workboat Code Edition 3: The Safety of Small Workboats and Pilot Boats – A Code of Practice</a>	MCA	2023
<a href="#">CAP 3038: Delivering Scalable UAS BVLOS in the Specific Category - The UK CAA Technical Strategy Delivery Model</a>	UK CAA	2024
<a href="#">GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY</a>	ENISA	2023
<a href="#">NIST Cybersecurity Framework</a>	NIST	2024
<a href="#">Out of the box – Implementing autonomy and assuring AI in the maritime industry</a>	Lloyd's Register	2023
<a href="#">NI641 RO1: Guidelines for autonomous shipping</a>	BV	2019
<a href="#">MGN 702</a>	MCA	2025
<a href="#">MGN 705</a>	MCA	2024
<a href="#">National Oceanography Centre (NOC) – Written evidence (AUV0056)</a>	NOC	2016
<a href="#">Industry Code of Conduct for Maritime Autonomous Systems</a>	UK MIA	2020
<a href="#">NIS2 Directive</a>	EU	2022
<a href="#">Cyber Assessment Framework</a>	NCSC	2024
<a href="#">GDPR</a>	EU	2016
<a href="#">10 Steps to Cyber Security Guidance</a>	NCSC	2021
<a href="#">Small Business Guide: Cyber Security</a>	NCSC	2020

## GLASGOW

### Inovo

ORE Catapult  
121 George Street  
Glasgow  
G1 1RD  
+44 (0) 333 004 1400

## BLYTH

### National Renewable Energy Centre

Offshore House  
Albert Street  
Blyth  
Northumberland  
NE24 1LZ  
+44 (0) 1670 359555

## LEVENMOUTH

### Levenmouth Development Turbine

Energy Park Fife  
Links Drive  
Leven  
Methil  
Fife  
KY8 3RA

## GRIMSBY

### O&M Centre of Excellence

ORE Catapult  
Port Office  
Cleethorpe Road  
Grimsby  
DN31 3LL

## ABERDEEN

### Floating Wind Innovation Centre (FLOWIC)

ORE Catapult  
W-Zero-1  
Energy Transition Zone  
Altens Industrial Estate  
Hareness Road  
Aberdeen  
AB12 3LE

## CORNWALL

### Hayle Marine Renewables Business Park

ORE Catapult  
North Quay  
Hayle  
Cornwall  
TR27 4DD

## PEMBROKESHIRE

### Marine Energy Engineering Centre of Excellence (MEECE)

Bridge Innovation Centre  
Pembrokeshire Science & Technology Park  
Pembroke Dock  
Wales  
SA72 6UN

## LOWESTOFT

### OrbisEnergy

ORE Catapult  
Wilde Street  
Lowestoft  
Suffolk  
NR32 1XH

### EMAIL US

[info@ore.catapult.org.uk](mailto:info@ore.catapult.org.uk)

### VISIT US

[ore.catapult.org.uk](http://ore.catapult.org.uk)

### ENGAGE WITH US

Instagram: [@ore.catapult](https://www.instagram.com/ore.catapult)

LinkedIn: [Offshore Renewable Energy Catapult](https://www.linkedin.com/company/offshore-renewable-energy-catapult)

Twitter: [@ORECatapult](https://twitter.com/ORECatapult)

YouTube: [@orecatapult](https://www.youtube.com/channel/UCq31111111111111111111)